REMARKS

The following remarks are fully and completely responsive to the Office Action dated October 6, 2004. Claims 1-8 are pending in this application with claims 1-3, 5-6 and 8 amended. In the outstanding Office Action, claims 1-8 were rejected under 35 U.S.C. § 102(b). No new matter has been added. Claims 1-8 are presented for reconsideration.

35 U.S.C. § 102(b)

Claims 1-8 were rejected under 35 U.S.C. § 102(b) as being anticipated by Blakley, III et al. (U.S. Patent No. 5,677,952). In making this rejection, the Office Action asserts that this reference teaches each and every element of the claimed invention. Applicant requests reconsideration of this rejection.

Claim 1 recites in part:

> requiring the entry into the device of the passphrase when a user wishes to access the data;
>
> subsequently inhibiting access to the data whilst the device remains active; and
>
> requiring the entry into the device of a predefined password when a user wishes to access the data following inhibition of data access, the password being different from the passphrase, wherein, if the user fails to enter the correct password within a predefined number of attempts, the cryptographic key stored by the device is deleted or re-encrypted.

Claim 5 recites in part:

receiving an entered passphrase and using the passphrase to generate or access a cryptographic key;

storing the cryptographic key in a memory of the device, wherein the stored key can be used to subsequently encrypt and decrypt data on the device;

subsequently inhibiting a user from accessing data on the device after a predefined period, or after a predefined period of non-use, or after some predefined action by the user;

requesting a user to input a password into the device;

receiving the password and, only if the password corresponds to a predefined password which is different from said passphrase, allowing the user to access data on the device, otherwise deleting or re-encrypting the cryptographic key.

Claim 6 recites in part:

first processing means for encrypting data using a cryptographic key derivable from or accessed using a passphrase;

input means for receiving the passphrase from a user when the user wishes to access the data; and

second processing means for subsequently inhibiting access to the data whilst the device remains active, and for requiring the entry into the device of a predefined password via said input means when a user wishes to access the data, the password being different from the passphrase, and for causing the cryptographic key stored by the device to be deleted or re-encrypted if the user fails to enter the correct password within a predefined number of attempts.

Claim 8 recites in part:

encrypting the data using a cryptographic key derivable from or accessed using a passphrase, requiring the entry into the device of the passphrase when a user wishes to access the data, subsequently inhibiting access to the data whilst the device remains active, and requiring the entry into the device of a predefined password when a user wishes to access the data,

the password being different from the passphrase, and, in the event that the user fails to enter the correct password within a predefined number of attempts, deleting or re-encrypting the cryptographic key stored by the device.

In contrast, Blakley teaches a method of securing data on a storage disk by encrypting the data using a pseudo-random function f which is applied to a secret key a and a disk sector number i which is the location at which the data is to be stored, i.e. fa(i). The data y to be encrypted and stored is XORed with the evaluated function, i.e. yXORfa(i). The secret key a is itself evaluated by applying a hash function to a user entered password Pu. This password serves a similar function to the passphrase recited in the present claims. Blakley states (see column 6, lines 53 to 57) that the efficient representation of fa, derived from the password Pu, is deleted at log-off, power-off, computer lock, or when a predetermined timeout occurs. When this happens, the user must re-enter the password when the computer is "restarted". Consequently, Blakley provides only a single layer of security -- the password.

However, the claimed invention requires the user to input both a passphrase and a password, which are specified as being different. In the embodiment described in detail in our application, the passphrase is assumed to be relatively long (providing a high degree of security or "entropy"), whilst the password is relatively short, e.g. a four digit PIN.

The Office Action correctly equates Blakley's password with the recited passphrase. The Office Action, however, incorrectly equates the recited password with a file name or user “click”.

Blakley uses the file name or user "click" to identify or select data to be encrypted (or decrypted). In contrast, the password recited in the present claims is used to access the data in an electronic device after access has been inhibited. Consequently, the password provides a second layer of security that is not disclosed or suggested by Blakley.

Additionally, Blakley fails to disclose or suggest inhibiting access to the data whilst the device remains active. In Blakley, if a timeout occurs (or the computer shut down), the function fa is deleted and no record of the password Pu is retained. To re-access the encrypted data, the password must be re-entered. In the claimed invention, however, if a timeout occurs activating the password entry function, a second low level security function is activated. Consequently, there is no equivalent second layer security in the method of Blakley.

Furthermore, the second, password-based security layer is linked to the first, passphrase-based security layer by deleting (or re-encrypting) the cryptographic key in the event that the user does not correctly enter the password when requested. This feature causes the security level to revert to the higher level, i.e. based on the assumption that if the password has not been correctly entered after some predefined number of tries, an attack is taking place.

If we equate the file name or user click of Blakley with our second level security password, there is nothing in Blakley to suggest that some incorrect user input will cause deletion or re-encryption of the encryption key (according to Blakley, we might consider his encryption key to be fa). Indeed, Blakley would merely act upon this mistaken entry and encrypt or decrypt the wrong file.

Consequently, the claimed invention provides a significant enhancement to the method of Blakley and to similar single level security systems. It maintains a high level of security for devices which are not in active use (and therefore possibly out of site of the owner), a low level security for devices which are in use, and a fallback to the high level in the event that an attack is suspected.

Therefore, Blakley fails to teach and/or suggest the claimed invention. Regarding claim 1, this reference fails to teach and/or suggest "subsequently inhibiting access to the data whilst the device remains active; and requiring the entry into the device of a predefined password when a user wishes to access the data following inhibition of data access, the password being different from the passphrase, wherein, if the user fails to enter the correct password within a predefined number of attempts, the cryptographic key stored by the device is deleted or re-encrypted".

Regarding claim 5, this reference fails to teach and/or suggest "subsequently inhibiting a user from accessing data on the device after a predefined period, or after a predefined period of non-use, or after some predefined action by the user; requesting a user to input a password into the device; receiving the password and, only if the password corresponds to a predefined password which is different from said passphrase, allowing the user to access data on the device, otherwise deleting or re-encrypting the cryptographic key".

Regarding claim 6, this reference fails to teach and/or suggest "second processing means for subsequently inhibiting access to the data whilst the device remains active, and for requiring the entry into the device of a predefined password via

said input means when a user wishes to access the data, the password being different from the passphrase, and for causing the cryptographic key stored by the device to be deleted or re-encrypted if the user fails to enter the correct password within a predefined number of attempts".

Regarding claim 8, this reference fails to teach and/or suggest "subsequently inhibiting access to the data whilst the device remains active, and requiring the entry into the device of a predefined password when a user wishes to access the data, the password being different from the passphrase, and, in the event that the user fails to enter the correct password within a predefined number of attempts, deleting or re-encrypting the cryptographic key stored by the device". Therefore, Applicant requests reconsideration and withdrawal of the rejection of claims 1-8 under 35 U.S.C. §102(b).

Conclusion

Applicant's remarks have overcome the objections and rejection set forth in the Office Action dated October 6, 2004. Applicant's remarks have distinguished claims 1, 5, 6 and 8 from Blakley and thus overcome the rejection of claims 1-8 under 35 U.S.C. §102(b). Accordingly, claims 1-8 are in condition for allowance. Therefore, Applicant respectfully requests consideration and allowance of claims 1-8.

Applicant submits that the application is now in condition for allowance. If the Examiner believes the application is not in condition for allowance, Applicant respectfully requests that the Examiner contact the undersigned attorney by telephone if it is believed that such contact will expedite the prosecution of the application.

In the event that this paper is not considered to be timely filed, Applicant hereby petitions for an appropriate extension of time. The Commissioner is authorized to charge payment for any additional fees which may be required with respect to this paper to our Deposit Account No. 01-2300, making reference to attorney docket number 108347-00011.

Respectfully submitted,
ARENT FOX PLLC

Rustan J. Hill
Registration No. 37,351

Customer No. 004372
ARENT FOX PLLC
1050 Connecticut Avenue, N.W.,
Suite 400
Washington, D.C. 20036-5339
Tel: (202) 857-6000
Fax: (202) 638-4810

RJH/elp
279576_1.DOC